

COUNTING POLYNOMIAL SUBSET SUMS

JIYOU LI AND DAQING WAN

ABSTRACT. Let D be a subset of a finite commutative ring R with identity. Let $f(x) \in R[x]$ be a polynomial of positive degree d . For integer $0 \leq k \leq |D|$, we study the number $N_f(D, k, b)$ of k -subsets $S \subseteq D$ such that

$$\sum_{x \in S} f(x) = b.$$

In this paper, we establish several asymptotic formulas for $N_f(D, k, b)$, depending on the nature of the ring R and f .

For $R = \mathbb{Z}_n$, let $p = p(n)$ be the smallest prime divisor of n , $|D| = n - c \geq C_d np^{-\frac{1}{d}} + c$ and $f(x) = a_d x^d + \cdots + a_0 \in \mathbb{Z}[x]$ with $(a_d, \dots, a_1, n) = 1$. Then

$$\left| N_f(D, k, b) - \frac{1}{n} \binom{n-c}{k} \right| \leq \binom{\delta(n)(n-c) + (1-\delta(n))(C_d np^{-\frac{1}{d}} + c) + k - 1}{k},$$

partially answering an open question raised by Stanley [25], where $\delta(n) = \sum_{i|n, \mu(i)=-1} \frac{1}{i}$ and $C_d = e^{1.85d}$. Furthermore, if n is a prime power, then $\delta(n) = 1/p$ and one can take $C_d = 4.41$.

For $R = \mathbb{F}_q$ of characteristic p , let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree d not divisible by p and $D \subseteq \mathbb{F}_q$ with $|D| = q - c \geq (d-1)\sqrt{q} + c$. Then

$$\left| N_f(D, k, b) - \frac{1}{q} \binom{q-c}{k} \right| \leq \binom{\frac{q-c}{p} + \frac{p-1}{p}((d-1)q^{\frac{1}{2}} + c) + k - 1}{k}.$$

If $f(x) = ax + b$, then this problem is precisely the well-known subset sum problem over a finite abelian group. Let G be a finite abelian group and let $D \subseteq G$ with $|D| = |G| - c \geq c$. Then

$$\left| N_x(D, k, b) - \frac{1}{|G|} \binom{|G|-c}{k} \right| \leq \binom{c + (|G| - 2c)\delta(e(G)) + k - 1}{k},$$

where $e(G)$ is the exponent of G and $\delta(n) = \sum_{i|n, \mu(i)=-1} \frac{1}{i}$. In particular, we give a new short proof for the explicit counting formula for the case $D = G$.

1. INTRODUCTION

Let D be a subset of a finite commutative ring R with identity. Let $f(x) \in R[x]$ be a polynomial of degree d . Many problems from combinatorics and number theory are reduced to computing the number $N_f(D, k, b)$, which is defined as the number of k -subsets $S \subseteq D$ such that

$$\sum_{x \in S} f(x) = b.$$

For example, when R equals \mathbb{Z}_n , this problem was raised by Stanley [25] (Page 136).

When $f(x)$ is linear, we may just take $f(x) = x$. The definition of $N(D, k, b) := N_x(D, k, b)$ is then defined for $R = G$ to be any finite abelian group (no ring structure is used). The problem of computing $N(D, k, b)$ is then reduced to the counting version of the k -subset sum problem over G .

For $G = \mathbb{Z}_n$, this problem is a well known **NP**-hard problem in theoretical computer science. For a general finite abelian group G , and an arbitrary $D \subseteq G$, determining if $N(D, k, b) > 0$ is an important difficult problem in algorithms and complexity. This has been studied extensively in recent years, especially over finite fields and over the group of rational points on an elliptic curve over a finite field, because of their important applications in coding theory and cryptography, see [4], [29], [31] and the references there. One expects that the problem is easier if $|D|$ is large compared to $|G|$ or D has some algebraic structure. For example, the dynamic programming algorithm gives a polynomial time algorithm to compute $N(D, k, b)$ if $|D| > |G|^\epsilon$ for some positive constant $\epsilon > 0$. In the extreme case that $D = G$, an explicit formula for $N(D, k, b)$ was obtained in Li and Wan [21], see also Kesters [16] for a new proof and an improvement. The sieving argument in [21] has been used to obtain a good asymptotic formula for $N(D, k, b)$ in the more general case that D is close to G , for instance, when $|D| \geq \frac{2}{3}|G|$. In the case that G is the group of rational points on an elliptical curve over a finite field, please refer to [22] for a concrete example.

For $G = \mathbb{Z}_n$, the finite cyclic group of n elements and $D = G = \mathbb{Z}_n$, an old result of Ramanathan (1945) gives an explicit formula for $N(\mathbb{Z}_n, k, b)$ by using equalities involving Ramanujan's trigonometric sums. A formula for $\sum_k N(D, k, b)$ and several generalizations were given by Stanley and Yoder [26], Kitchloo and Patcher [17].

When $G = \mathbb{Z}_p$ is the finite cyclic group of prime order p and $|D| \gg p^{2/3}$ is arbitrary, Erdős and Heilbronn proved in their famous paper [8] that $\sum_k N(D, k, b) = \frac{2p}{p}(1 + o(1))$ when p tends to infinity.

When G is the additive group of a finite field \mathbb{F}_q and $|G| - |D|$ is bounded by a constant, an explicit formula for $N(D, k, b)$ was given in [19]. When G is an arbitrary finite abelian group, and $D = G$ or $D = G^*$, an explicit and efficiently computable formula for $N(D, k, b)$ was given in [21]. Kesters [14] gave a different and shorter proof by using methods of group rings. In this paper, we will give a third short proof.

We also obtain a general bound for the k -subset sum problem over G , which significantly generalizes previous results which assumed D to be very close to G . This will be explained shortly later for the case $|G| = p$.

Theorem 1.1. *Let G be a finite abelian group of order $|G|$. Let $D \subseteq G$ with $|D| = |G| - c \geq c$. Let $N(D, k, b)$ be the number of k -subsets in D which sums to b . Then*

$$\left| N(D, k, b) - \frac{1}{|G|} \binom{|G| - c}{k} \right| \leq \left(c + (|G| - 2c) \left(\sum_{i|e(G), \mu(i)=-1} \frac{1}{i} \right) + k - 1 \right),$$

where $e(G)$ is the exponent of G , which is defined as the maximal order of a nonzero element in G .

In order for this bound to be non-trivial, at least k and c need to satisfy

$$|G| - c > (|G| - 2c) \left(\sum_{i|e(G), \mu(i)=-1} \frac{1}{i} \right) + k + c.$$

Corollary 1.2. *Let G be a finite elementary abelian p -group (thus $e(G) = p$). Then,*

$$\left| N(D, k, b) - \frac{1}{|G|} \binom{|G| - c}{k} \right| \leq \binom{\frac{(|G| - 2c)}{p} + c + k - 1}{k}.$$

In the case $|G| = p$, to obtain a non-trivial estimate, one needs to solve

$$p - c > \frac{(p - 2c)}{p} + k + c.$$

Asymptotically, for smaller k , we could take c as large as $p/2$.

Let us turn to the cases for general $f(x)$. Few results are known for the number $N_f(D, k, b)$ when $f(x)$ is a polynomial of higher degree. In the case that $f(x)$ is the simplest monomial x^d , R is the prime field \mathbb{F}_p and $D = \mathbb{F}_p^*$, it was first proved by Odlyzko-Stanley [24] that

$$\left| N_{x^d}(\mathbb{F}_p^*, b) - \frac{2^{p-1}}{p} \right| \leq e^{O(d\sqrt{p} \log p)},$$

where $N_{x^d}(\mathbb{F}_p^*, b) = \sum_{k=0}^{p-1} N_{x^d}(\mathbb{F}_p^*, k, b)$.

For a general finite field $R = \mathbb{F}_q$, the finite field of $q = p^t$ elements, Zhu and Wan [30] proved the following more precise result:

$$\left| N_{x^d}(\mathbb{F}_q^*, k, b) - \frac{1}{q} \binom{q-1}{k} \right| \leq 2q^{-1/2} \binom{d\sqrt{q} + q/p + k}{k}.$$

Since $N_{x^d}(\mathbb{F}_q^*, b) = \sum_{k=0}^{q-1} N_{x^d}(\mathbb{F}_q^*, k, b)$, one can then deduce the following explicit bound

$$\left| N_{x^d}(\mathbb{F}_q^*, b) - \frac{2^{q-1}}{q} \right| \leq \frac{4p}{\sqrt{2\pi q}} e^{(d\sqrt{q} + q/p) \log q},$$

which extends the Odlyzko-Stanley bound from a prime finite field to a general finite field. Note that simply replacing p with q in the Odlyzko-Stanley bound is not known to be true and is probably not true if q is a high power of p . It is true if $q = p^2$.

These bounds are nontrivial only for $d \leq \sqrt{q}$. When $q = p$ is prime, a series of subsequent work had been made by Garcia-Voloch, Shparlinski, Heath-Brown, Heath-Brown-Konyagin and Konyagin. They used variations of Stepanov's method and released the limit on the degree to $d \leq p^{3/4-\epsilon}$. For more details, please refer to [1]. Using their remarkable Gauss sum bound proved by using additive combinatorics and harmonic analysis, Bourgain, Glibichuk and Konyagin [2, 3] proved that if $d < p^{1-\delta}$ for some constant $\delta > 0$, then there is a constant $0 < \epsilon = \epsilon(\delta) < \delta$ such that

$$\left| N_{x^d}(\mathbb{F}_p^*, b) - \frac{2^{p-1}}{p} \right| \leq e^{O(p^{1-\epsilon})}.$$

By combining Bourgain's bound and Li and Wan's sieving technique [20], Li [18] proved a refined result that if $d < p^{1-\delta}$, then there is a constant $0 < \epsilon = \epsilon(\delta) < \delta$ such that

$$\left| N_{x^d}(\mathbb{F}_p^*, k, b) - \frac{1}{p} \binom{p-1}{k} \right| \leq \binom{p^{1-\epsilon} + dk - d}{k}.$$

It would be interesting to extend this type of result to a general finite field of characteristic p .

In this paper, we obtain several asymptotic formulas for $N_f(D, k, b)$ when $f(x)$ is a general higher degree polynomial. In the case that $R = \mathbb{Z}_n$, the finite ring of n residues mod n , and f is a polynomial of degree d over the integers, we have the following bound, proved using Hua's bound for exponential sums and our sieving technique.

Theorem 1.3. *Let $R = \mathbb{Z}_n$ and $p = p(n)$ be the smallest prime divisor of n . Assume $|D| = n - c \geq C_d n p^{-\frac{1}{d}} + c$ and $f(x) = a_d x^d + \dots + a_0 \in \mathbb{Z}[x]$ with $(a_d, \dots, a_1, n) = 1$. Then we have*

$$\left| N_f(D, k, b) - \frac{1}{n} \binom{n-c}{k} \right| \leq \binom{\delta(n)(n-c) + (1-\delta(n))(C_d n p^{-\frac{1}{d}} + c) + k - 1}{k},$$

where $\delta(n) = \sum_{i|n, \mu(i)=-1} \frac{1}{i}$ and $C_d = e^{1.85d}$. Furthermore, if n is a prime power, then $\delta(n) = 1/p$ and the constant $e^{1.85d}$ can be improved to the absolute constant 4.41.

Note that the above bound is pretty good for n with only large prime factors so that $\delta(n) = \sum_{i|n, \mu(i)=-1} \frac{1}{i}$ is relatively small.

When $R = \mathbb{F}_q$ and f is a polynomial of degree d over \mathbb{F}_q , we obtain a better bound thanks to the Weil bound. In this case, for simplicity, we suppose that $f(x) \in \mathbb{F}_q[x]$ is a polynomial of degree d , d is not divisible by p and $d < q$ since $x^q = x$ for all $x \in \mathbb{F}_q$.

Theorem 1.4. *Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree d not divisible by p . For $R = \mathbb{F}_q$ and $|D| = q - c \geq (d-1)\sqrt{q} + c$, we have*

$$\left| N_f(D, k, b) - \frac{1}{q} \binom{q-c}{k} \right| \leq \binom{\frac{q-c}{p} + \frac{p-1}{p}((d-1)q^{\frac{1}{2}} + c) + k - 1}{k}.$$

In particular, if $q = p$ is a prime, then we have a nice “quadratic root” bound.

Corollary 1.5. *Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree $0 < d < p$. For $R = \mathbb{F}_p$ and $|D| = p - c \geq (d-1)\sqrt{p} + c$, we have*

$$\left| N_f(D, k, b) - \frac{1}{p} \binom{p-c}{k} \right| \leq \binom{(d-1)p^{\frac{1}{2}} + c + k}{k}.$$

The paper is organized as follows. In Section 2, we briefly review a distinct coordinate sieving formula. In Section 3, we establish a general formula for general ring R . In the remaining sections, several more explicit formula are derived.

Notations. For $x \in \mathbb{R}$, let $(x)_0 = 1$ and $(x)_k = x(x-1)\dots(x-k+1)$ for $k \in \mathbb{Z}^+$. For $k \in \mathbb{N}$, $\binom{x}{k}$ is the binomial coefficient defined by $\binom{x}{k} = \frac{(x)_k}{k!}$. For a power series $f(x)$, $[x^k]f(x)$ denotes the coefficient of x^k in $f(x)$. $[x]$ always denotes the largest integer not greater than x .

2. A DISTINCT COORDINATE SIEVING FORMULA

For the purpose of our proof, we briefly introduce the sieving formula discovered by Li and Wan [20]. Roughly speaking, this formula significantly improves the classical inclusion-exclusion sieve for distinct coordinate counting problems. We cite it here without proof. The first proof of this formula was given in [20]. For a different proof by the theory of partial order please refer to [21].

Let Ω be a finite set, and let Ω^k be the Cartesian product of k copies of Ω . Let X be a subset of Ω^k . Define $\overline{X} = \{(x_1, x_2, \dots, x_k) \in X \mid x_i \neq x_j, \forall i \neq j\}$. Denote S_k to be the symmetric group on k elements. For a permutation τ in S_k , the sign of τ is defined by $\text{sign}(\tau) = (-1)^{k-l(\tau)}$, where $l(\tau)$ is the number of cycles of τ including the trivial ones. Suppose we have the factorization $\tau = (i_1 i_2 \dots i_{a_1})(j_1 j_2 \dots j_{a_2}) \dots (l_1 l_2 \dots l_{a_s})$ with $1 \leq a_i, 1 \leq i \leq s$, then define

$$X_\tau = \{(x_1, \dots, x_k) \in X, x_{i_1} = \dots = x_{i_{a_1}}, \dots, x_{l_1} = \dots = x_{l_{a_s}}\}. \quad (2.1)$$

Now we will state our sieve formula. We notice that there are many other interesting corollaries of this formula [20, 21].

Theorem 2.1. *Let $f(x_1, x_2, \dots, x_k)$ be any complex valued function defined over X . Then*

$$\sum_{x \in \overline{X}} f(x_1, x_2, \dots, x_k) = \sum_{\tau \in S_k} \text{sign}(\tau) \sum_{x \in X_\tau} f(x_1, x_2, \dots, x_k).$$

Note that in many situations the sum $\sum_{x \in X_\tau} f(x_1, x_2, \dots, x_k)$ is much easier to compute compared to the left one.

S_k acts on Ω^k naturally by permuting the coordinates. That is, for $\tau \in S_k$ and $x = (x_1, x_2, \dots, x_k) \in \Omega^k$, $\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(k)})$. A subset X in Ω^k is said to be symmetric if for any $x \in X$ and any $\tau \in S_k$, $\tau \circ x \in X$. For $\tau \in S_k$, denote by $\overline{\tau}$ the conjugacy class represented by τ and sometimes it is more convenient to view it as the set of permutations conjugate to τ . Conversely, for a conjugacy class $\overline{\tau} \in C_k$, just let τ denote a representative permutation in this class.

In particular, since two permutations in S_k are conjugate if and only if they have the same type of cycle structure, if X is symmetric and f is a symmetric function under the action of S_k , then we have the following simpler formula.

Corollary 2.2. *Let C_k be the set of conjugacy classes of S_k . If X is symmetric and f is symmetric, then*

$$\sum_{x \in \overline{X}} f(x_1, x_2, \dots, x_k) = \sum_{\overline{\tau} \in C_k} \text{sign}(\tau) C(\tau) \sum_{x \in X_\tau} f(x_1, x_2, \dots, x_k), \quad (2.2)$$

where $C(\tau)$ is the number of permutations conjugate to τ .

Lemma 2.3. *We have the following inequality for the coefficients of rational functions. For positive integers m and n ,*

$$[x^k] \frac{1}{(1-x^m)^n} \leq [x^k] \frac{1}{(1-x)^n}.$$

Proof. Since

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \binom{k+n-1}{k} x^k,$$

we have

$$[x^k] \frac{1}{(1-x^m)^n} \leq \binom{[k/m] + n - 1}{[k/m]} \leq \binom{k+n-1}{k} = [x^k] \frac{1}{(1-x)^n}.$$

□

Lemma 2.4. *If for all integers $k \geq 0$, we have*

$$[x^k]f_1(x) \leq [x^k]g_1(x), \quad [x^k]f_2(x) \leq [x^k]g_2(x),$$

then for all integers $k \geq 0$,

$$[x^k]f_1(x)f_2(x) \leq [x^k]g_1(x)g_2(x).$$

Proof.

$$[x^k]f_1(x)f_2(x) = \sum_{i=0}^k [x^i]f_1(x) \cdot [x^{k-i}]f_2(x) \leq \sum_{i=0}^k [x^i]g_1(x) [x^{k-i}]g_2(x) = [x^k]g_1(x)g_2(x).$$

□

Lemma 2.5. *If a, b are integers and $0 \leq b \leq a$, then we have the inequality on the coefficients for rational functions.*

$$[x^k] \frac{(1 - x^{pq})^b}{(1 - x^p)^a} \leq [x^k] \frac{1}{(1 - x^p)^a}.$$

Proof. Applying Lemma 2.3 and Lemma 2.4, we have

$$\begin{aligned} [x^k] \frac{(1 - x^{pq})^b}{(1 - x^p)^a} &= [x^k] \left(\frac{1 - x^{pq}}{1 - x^p} \right)^b \cdot \frac{1}{(1 - x^p)^{a-b}} \\ &= [x^k] (1 + x^p + \cdots + x^{(q-1)p})^b \cdot \frac{1}{(1 - x^p)^{a-b}} \\ &\leq [x^k] (1 + x^p + \cdots + x^{(q-1)p} + \cdots)^b \cdot \frac{1}{(1 - x^p)^{a-b}} \\ &= [x^k] \frac{1}{(1 - x^p)^a}. \end{aligned}$$

□

We now establish a combinatorial upper bound which is crucial for the proof of our main results. A permutation $\tau \in S_k$ is said to be of type (c_1, c_2, \dots, c_k) if τ has exactly c_i cycles of length i . Note that $\sum_{i=1}^k ic_i = k$. Let $N(c_1, c_2, \dots, c_k)$ be the number of permutations in S_k of type (c_1, c_2, \dots, c_k) . It is well known that

$$N(c_1, c_2, \dots, c_k) = \frac{k!}{1^{c_1} c_1! 2^{c_2} c_2! \cdots k^{c_k} c_k!},$$

and we then define the generating function

$$C_k(t_1, t_2, \dots, t_k) = \sum_{\sum ic_i = k} N(c_1, c_2, \dots, c_k) t_1^{c_1} t_2^{c_2} \cdots t_k^{c_k}.$$

Lemma 2.6. *Let $q \geq s$ be two positive real numbers. If $t_i = q$ for $(i, d) > 1$ and $t_i = s$ for $(i, d) = 1$, then we have the bound*

$$\begin{aligned} C_k(\overbrace{s, \dots, s}^{(i,d)=1}, \overbrace{s, \dots, s}^{(i,d)=1}, q, \dots) &= \sum_{\sum ic_i = k} N(c_1, c_2, \dots, c_k) s^{c_1} s^{c_2} \cdots q^{c_d} s^{c_{d+1}} \cdots \\ &\leq (s + (q - s) \left(\sum_{i|d, \mu(i)=-1} \frac{1}{i} \right) + k - 1)_k. \end{aligned}$$

Proof. Suppose d has the prime factorization $d = \prod_{j=1}^t p_j^{s_j}$. By the definition of the exponential generating function, we have

$$\sum_{k \geq 0} C_k(t_1, t_2, \dots, t_k) \frac{u^k}{k!} = e^{ut_1 + u^2 \cdot \frac{t_2}{2} + u^3 \cdot \frac{t_3}{3} + \dots}.$$

By the conditions $t_i = q$ for $(i, d) > 1$ and $t_i = s$ for $(i, d) = 1$, we deduce

$$\begin{aligned} C_k(\overbrace{s, \dots, s}^{(i,d)=1}, q, \overbrace{s, \dots, s}^{(i,d)=1}, q, \dots) &= \left[\frac{u^k}{k!} \right] e^{us + u^2 \cdot \frac{s}{2} + \dots + u^{d-1} \cdot \frac{s}{d-1} + u^d \cdot \frac{q}{d} + u^{d+1} \cdot \frac{s}{d+1} + \dots} \\ &= \left[\frac{u^k}{k!} \right] e^{s \sum_i \frac{u^i}{i} + (q-s) \sum_{(i,d) > 1} \frac{u^i}{i}}. \end{aligned}$$

Using the inclusion-exclusion, the above expression can be re-written as

$$\begin{aligned} & \left[\frac{u^k}{k!} \right] e^{s \sum_i \frac{u^i}{i} + (q-s) \left(\sum_{p_1 | i} \frac{u^i}{i} + \sum_{p_2 | i} \frac{u^i}{i} + \dots - \sum_{p_1 p_2 | i} \frac{u^i}{i} - \dots \right)} \\ &= \left[\frac{u^k}{k!} \right] e^{-s \log(1-u) - \frac{q-s}{p_1} \log(1-u^{p_1}) - \frac{q-s}{p_2} \log(1-u^{p_2}) - \dots + \frac{q-s}{p_1 p_2} \log(1-u^{p_1 p_2}) + \dots} \\ &= \left[\frac{u^k}{k!} \right] \frac{(1-u^{p_1 p_2})^{\frac{q-s}{p_1 p_2}} \dots}{(1-u)^s (1-u^{p_1})^{\frac{q-s}{p_1}} (1-u^{p_2})^{\frac{q-s}{p_2}} \dots} \\ &\leq \left[\frac{u^k}{k!} \right] \frac{1}{(1-u)^s (1-u^{p_1})^{\frac{q-s}{p_1}} (1-u^{p_2})^{\frac{q-s}{p_2}} \dots (1-u^{p_1 p_2 p_3})^{\frac{q-s}{p_1 p_2 p_3}} \dots} \\ &\leq \left[\frac{u^k}{k!} \right] \frac{1}{(1-u)^s (1-u)^{\frac{q-s}{p_1}} (1-u)^{\frac{q-s}{p_2}} \dots (1-u)^{\frac{q-s}{p_1 p_2 p_3}} \dots} \\ &= k! \binom{s + (q-s) \left(\sum_{i|d, \mu(i)=-1} \frac{1}{i} \right) + k - 1}{k} \\ &= (s + (q-s) \left(\sum_{i|d, \mu(i)=-1} \frac{1}{i} \right) + k - 1)_k. \end{aligned}$$

In the above inequality step, we used Lemma 2.5 and Lemma 2.3. \square

In the same spirit, a simpler special case is the following lemma and the proof is omitted.

Lemma 2.7. *Let $q \geq s$ be two non negative real numbers. If $t_i = q$ for $d \mid i$ and $t_i = s$ for $d \nmid i$, then we have*

$$\begin{aligned} C_k(\overbrace{s, \dots, s}^{d \nmid i}, q, \overbrace{s, \dots, s}^{d \nmid i}, q, \dots) &= \sum_{\sum i c_i = k} N(c_1, c_2, \dots, c_k) s^{c_1} s^{c_2} \dots q^{c_d} s^{c_{d+1}} \dots \\ &= \left[\frac{u^k}{k!} \right] \frac{1}{(1-u)^s (1-u^d)^{\frac{q-s}{d}}}. \\ &\leq \left[\frac{u^k}{k!} \right] \frac{1}{(1-u)^s (1-u)^{\frac{q-s}{d}}} \\ &= (s + (q-s)/d + k - 1)_k. \end{aligned}$$

3. GENERAL CASE R

Let ψ denote an additive character from $G = (R, +)$, the additive group of R , to the group of all nonzero complex numbers \mathbb{C}^* . Let ψ_0 be the principal character sending each element in G to 1. Denote by \hat{G} the group of additive characters of G , which is isomorphic to G .

Lemma 3.1. *Suppose that $|R| = q$ and $D \subseteq R$ with $|D| = m$. For a fixed polynomial $f(x) \in R[x]$, let $N_f(D, k, b)$ be the number of k -subsets $S \subseteq D$ such that $\sum_{x \in S} f(x) = b$. Then*

$$k!N_f(D, k, b) = \frac{1}{q}(m)_k + \frac{1}{q} \sum_{\psi \neq \psi_0} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi),$$

where C_k is the set of all conjugacy classes of S_k and $C(\tau)$ counts the number of permutations conjugate to τ , and

$$F_\tau(\psi) = \prod_{i=1}^k \left(\sum_{a \in D} \psi^i(f(a)) \right)^{c_i}.$$

Proof. Let $X = D \times D \times \cdots \times D$ be the Cartesian product of k copies of D . Define $\overline{X} = \{(x_1, x_2, \dots, x_k) \in D^k \mid x_i \neq x_j, \forall i \neq j\}$ to be the set of all distinct configurations in X . It is clear that $|X| = m^k$ and $|\overline{X}| = (m)_k$. Applying the orthogonal relations of the characters, one deduces that

$$\begin{aligned} k!N_f(D, k, b) &= \frac{1}{q} \sum_{(x_1, x_2, \dots, x_k) \in \overline{X}} \sum_{\psi \in \hat{G}} \psi(f(x_1) + f(x_2) + \cdots + f(x_k) - b) \\ &= \frac{1}{q}(m)_k + \frac{1}{q} \sum_{\psi \neq \psi_0} \psi^{-1}(b) \sum_{(x_1, x_2, \dots, x_k) \in \overline{X}} \prod_{i=1}^k \psi(f(x_i)). \end{aligned}$$

For $\psi \neq \psi_0$, let $f_\psi(x) = f_\psi(x_1, x_2, \dots, x_k) = \prod_{i=1}^k \psi(f(x_i))$. For $\tau \in S_k$, let

$$F_\tau(\psi) = \sum_{x \in X_\tau} f_\psi(x) = \sum_{x \in X_\tau} \prod_{i=1}^k \psi(f(x_i)),$$

where X_τ is defined as in equation (2.1). Obviously X is symmetric and $f_\psi(x_1, x_2, \dots, x_k)$ is also symmetric on X . Applying equation (2.2) in Corollary 2.2, we have

$$k!N_f(D, k, b) = \frac{1}{q}(m)_k + \frac{1}{q} \sum_{\psi \neq \psi_0} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi),$$

where C_k is the set of all conjugacy classes of S_k and $C(\tau)$ counts the number of permutations conjugate to τ . For $\tau \in C_k$, assume τ is of type (c_1, c_2, \dots, c_k) , where c_i is the number of i -cycles in τ for $1 \leq i \leq k$. Note that $\sum_{i=1}^k i c_i = k$. Write

$$\tau = (i_1)(i_2) \cdots (i_{c_1})(i_{c_1+1} i_{c_1+2}) (i_{c_1+3} i_{c_1+4}) \cdots (i_{c_1+2c_2-1} i_{c_1+2c_2}) \cdots.$$

One checks that

$$X_\tau = \{(x_1, \dots, x_k) \in D^k, x_{i_{c_1+1}} = x_{i_{c_1+2}}, \dots, x_{i_{c_1+2c_2-1}} = x_{i_{c_1+2c_2}}, \dots\}.$$

Then we have

$$F_\tau(\psi) = \sum_{x \in X_\tau} \prod_{i=1}^k \psi(f(x_i))$$

$$\begin{aligned}
&= \sum_{x \in X_\tau} \prod_{i=1}^{c_1} \psi(f(x_i)) \prod_{i=1}^{c_2} \psi^2(f(x_{c_1+2i})) \cdots \prod_{i=1}^{c_k} \psi^k(f(x_{c_1+c_2+\cdots+ki})) \\
&= \prod_{i=1}^k \left(\sum_{a \in D} \psi^i(f(a)) \right)^{c_i}.
\end{aligned}$$

□

The above lemma reduces the study of the asymptotic formula for $N_f(D, k, b)$ to the estimate of the partial character sum $\sum_{a \in D} \psi(f(a))$ and another sum through ψ . This is very difficult in general. However, if either D is large compared to R , or D and $f(x)$ have some nice algebraic structures, one expects non-trivial estimates. One important example is the case that $D = \mathbb{F}_p^*$ and $f(x) = x^d$. As we have mentioned in the introduction section, a series of works by Garcia-Voloch, Heath Brown, Konyagin-Shparlinski, Konyagin using variants of Stepanov's method ($d < p^{3/4-\epsilon}$), and by Bourgain and Konyagin using additive combinatorics and harmonic analysis ($d < p^{1-\epsilon}$) shows that in this case D has a nice pseudo random property.

We are now ready to use the above lemma to prove our main results by estimating various partial character sums and different summations in different cases.

4. THE RESIDUE RING CASE $R = \mathbb{Z}_n$

We first recall the following results on character sums over the residue class ring.

Lemma 4.1 (Hua and Lu [11, 23]). *Suppose ψ is a primitive additive character of the group \mathbb{Z}_n . Let $f(x) = \sum_{i=0}^d a_i x^i \in \mathbb{Z}[x]$ be a polynomial of positive degree d . If $(a_1, \dots, a_d, n) = 1$, then*

$$\left| \sum_{x \in \mathbb{Z}_n} \psi(f(x)) \right| \leq e^{1.85d} n^{1-\frac{1}{d}}.$$

Thus if $D \subseteq \mathbb{Z}_n$ with $|D| = n - c$, then

$$\left| \sum_{x \in D} \psi(f(x)) \right| \leq e^{1.85d} n^{1-\frac{1}{d}} + c. \quad (4.1)$$

For $d \geq 3$, the bound (5.1) can be improved to

$$\left| \sum_{x \in \mathbb{Z}_n} \psi(f(x)) \right| \leq e^{1.74d} n^{1-\frac{1}{d}}.$$

by Ding and Qi [7]. See also Stečkin [27] for an asymptotically better but not explicit bound for large d .

When n is a prime power, Hua [11, 12, 13] first obtained the bound

$$\left| \sum_{x \in \mathbb{Z}_n} \psi(f(x)) \right| \leq d^3 n^{1-\frac{1}{d}},$$

and it was improved by many mathematicians including Chen, Chalk, Ding, Loh, Lu, Mit'kin, Nečaeu and Stečkin [6]. The current best bound is proved by Cochrane and Zheng.

Lemma 4.2 (Cochrane and Zheng, [5]). *Suppose ψ is a primitive additive character of the group \mathbb{Z}_n . Let $f(x) = \sum_{i=0}^d a_i x^i \in \mathbb{Z}[x]$ be a polynomial of positive degree d . Assume $n = p^t$ and $(a_1, \dots, a_d, p) = 1$. Then*

$$\left| \sum_{x \in \mathbb{Z}_n} \psi(f(x)) \right| \leq 4.41n^{1-\frac{1}{d}}.$$

Similarly, if $D \subseteq \mathbb{Z}_n$ with $|D| = n - c$, then

$$\left| \sum_{x \in D} \psi(f(x)) \right| \leq 4.41n^{1-\frac{1}{d}} + c.$$

For readers interested in the exponential sums over \mathbb{Z}_n , we refer to a good survey by Cochrane and Zheng [6].

Proof of Theorem for $R = \mathbb{Z}_n$. Let ψ_0 be the principal character sending each element in \mathbb{Z}_n to 1. Also denote by $\hat{\mathbb{Z}}_n$ the group of additive characters of \mathbb{Z}_n . Let $N_f(D, k, b)$ be the number of k -subsets $S \subseteq D$ such that $\sum_{x \in S} f(x) = b$. Write $|D| = m$. Applying Lemma 3.1, we have

$$k!N_f(D, k, b) = \frac{1}{n}(m)_k + \frac{1}{n} \sum_{\psi \in \hat{\mathbb{Z}}_n, \psi \neq \psi_0} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi),$$

where C_k is the set of all conjugacy classes of S_k and $C(\tau)$ counts the number of permutations conjugate to τ , and

$$F_\tau(\psi) = \prod_{i=1}^k \left(\sum_{a \in D} \psi^i(f(a)) \right)^{c_i}.$$

Let $C_d = e^{1.85d}$ for general n and $C_d = 4.41$ for prime power $n = p^t$. Applying equation 4.1 in Lemma 5.1, if ψ is primitive, then

$$|F_\tau(\psi)| \leq m^{\sum_{i=1}^k c_i m_i(\psi)} (C_d n^{1-\frac{1}{d}} + c)^{\sum_{i=1}^k c_i (1-m_i(\psi))},$$

where $m_i(\psi)$ is defined as follows: $m_i(\psi) = 1$ if $(i, n) > 1$ and $m_i(\psi) = 0$ if $(i, n) = 1$. Similarly, if $\text{order}(\psi) = h, h \mid n$, then

$$\left| \sum_{x \in \mathbb{Z}_n} \psi(f(x)) \right| = \frac{n}{h} \left| \sum_{x \in \mathbb{Z}_h} \psi(f(x)) \right| \leq C_d n h^{-\frac{1}{d}}.$$

Thus

$$|F_\tau(\psi)| \leq m^{\sum_{i=1}^k c_i m_i(\psi)} (C_d n h^{-\frac{1}{d}} + c)^{\sum_{i=1}^k c_i (1-m_i(\psi))},$$

where $m_i(\psi) = 1$ if $(i, h) > 1$ and $m_i(\psi) = 0$ if $(i, h) = 1$.

Let $p = p(n)$ be the smallest prime divisor of n . Assume

$$m \geq \max_{h \mid n, h \neq 1} \{C_d n h^{-\frac{1}{d}} + c\} = C_d n p^{-\frac{1}{d}} + c.$$

Then we have

$$\begin{aligned} k!N_f(D, k, b) &= \frac{1}{n}(m)_k + \frac{1}{n} \sum_{1 \neq h \mid n} \sum_{\psi, \text{order}(\psi)=h} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi) \\ &\geq \frac{1}{n}(m)_k - \frac{1}{n} \sum_{1 \neq h \mid n} \phi(h) \sum_{\tau \in C_k} C(\tau) m^{\sum_{j=1}^k c_j} (C_d n h^{-\frac{1}{d}} + c)^{\sum_{j=1, (h,j)>1}^k c_j} \end{aligned}$$

$$\geq \frac{1}{n}(m)_k - \frac{1}{n} \sum_{1 \neq h|n} \phi(t)(C_d n h^{-\frac{1}{d}} + c + (m - C_d n h^{-\frac{1}{d}} - c) \left(\sum_{i|h, \mu(i)=-1} \frac{1}{i} \right) + k - 1)_k$$

Define $\delta(h) = \sum_{i|h, \mu(i)=-1} \frac{1}{i}$. Obviously $\max\{\delta(h), h \mid n\} = \delta(n)$. Hence

$$\begin{aligned} k!N_f(D, k, b) &\geq \frac{1}{n}(m)_k - (C_d n p^{-\frac{1}{d}} + c + (m - C_d n p^{-\frac{1}{d}} - c)\delta(n) + k - 1)_k \\ &= \frac{1}{n}(m)_k - (\delta(n)m + (1 - \delta(n)(C_d n p^{-\frac{1}{d}} + c) + k - 1)_k. \end{aligned}$$

The second inequality follows from Lemma 2.6.

5. THE FINITE FIELD CASE $R = \mathbb{F}_q$

For our proof, we first recall Weil's character sum estimate in the following form [28].

Lemma 5.1 (Weil). *Suppose ψ is a non-trivial additive character of the additive group \mathbb{F}_q . Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree d not divisible by p . Then,*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(f(x)) \right| \leq (d-1)\sqrt{q}.$$

Corollary 5.2. *Suppose ψ is a non-trivial additive character of the additive group \mathbb{F}_q . Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree d not divisible by p . Suppose $D \subseteq \mathbb{F}_q$ and $|D| = q - c$. Then,*

$$\left| \sum_{x \in D} \psi(f(x)) \right| \leq (d-1)\sqrt{q} + c. \quad (5.1)$$

Proof of Theorem for $R = \mathbb{F}_q$. Write $|D| = m$. Applying Lemma 3.1, we have

$$k!N_f(D, k, b) = \frac{1}{q}(m)_k + \frac{1}{q} \sum_{\psi \neq \psi_0} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi),$$

where C_k is the set of all conjugacy classes of S_k and $C(\tau)$ counts the number of permutations conjugate to τ , and

$$F_\tau(\psi) = \prod_{i=1}^k \left(\sum_{a \in D} \psi^i(f(a)) \right)^{c_i}.$$

Applying equation 5.1 in Corollary 5.2, we have

$$|F_\tau(\psi)| \leq m^{\sum_{i=1}^k c_i m_i(\psi)} ((d-1)q^{\frac{1}{2}} + c)^{\sum_{i=1}^k c_i (1-m_i(\psi))},$$

where $m_i(\psi)$ is defined as follows: $m_i(\psi) = 1$ if $\psi^i = 1$ and $m_i(\psi) = 0$ if $\psi^i \neq 1$.

Since the additive group of \mathbb{F}_q is p -elementary, for nontrivial character ψ , $\text{order}(\psi) = p$. Thus $\psi^i = 1$ if and only if $p \mid i$. Assume $m \geq (d-1)q^{\frac{1}{2}} + c$. We deduce

$$\begin{aligned} k!N_f(D, k, b) &= \frac{1}{q}(m)_k + \frac{1}{q} \sum_{\psi, \text{order}(\psi)=p} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi) \\ &\geq \frac{1}{q}(m)_k - \frac{q-1}{q} \sum_{\tau \in C_k} C(\tau) m^{\sum_{j=1, p \nmid j}^k c_j} ((d-1)q^{\frac{1}{2}} + c)^{\sum_{j=1, p \nmid j}^k c_j} \end{aligned}$$

$$\geq \frac{1}{q}(m)_k - \left(\frac{m}{p} + \frac{p-1}{p}((d-1)q^{\frac{1}{2}} + c) + k-1\right)_k.$$

The last equality follows from Lemma 2.7 in the case that $d = p$.

6. THE CASE $f(x) = x$, $R = G$ AND $D \subseteq G$ ARBITRARY

Proof of Theorem for $R = G$. Let \hat{G} be the group of additive characters of G and let ψ_0 be the principal character sending each element in G to 1. Let $N(D, k, b)$ be the number of k -subsets $S \subseteq D$ such that $\sum_{x \in S} x = b$. Write $|G| = n$ and $|D| = m = n - c$. Suppose $m > c$. Applying Lemma 3.1, we have

$$k!N(D, k, b) = \frac{1}{n}(m)_k + \frac{1}{n} \sum_{\psi \neq \psi_0} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi),$$

where C_k is the set of all conjugacy classes of S_k and $C(\tau)$ counts the number of permutations conjugate to τ , and

$$F_\tau(\psi) = \prod_{i=1}^k \left(\sum_{a \in D} \psi^i(a) \right)^{c_i}.$$

A trivial character sum bound gives

$$|F_\tau(\psi)| \leq m^{\sum_{i=1}^k c_i m_i(\psi)} c^{\sum_{i=1}^k c_i (1-m_i(\psi))},$$

where $m_i(\psi)$ is defined as follows: $m_i(\psi) = 1$ if $\psi^i = 1$ and $m_i(\psi) = 0$ if $\psi^i \neq 1$.

Let $e(G)$ be the exponent of G and so it is also the exponent of \hat{G} . Thus for nontrivial character ψ , $m_i(\psi) = 0$ if $(e(G), i) = 1$. Since $m > c$, we have

$$\begin{aligned} k!N(D, k, b) &= \frac{1}{n}(m)_k + \frac{1}{n} \sum_{\psi \neq \psi_0} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi) \\ &\geq \frac{1}{n}(m)_k - \frac{n-1}{n} \sum_{\tau \in C_k} C(\tau) m^{\sum_{j=1, (e(G), j) > 1}^k c_j} c^{\sum_{j=1, (e(G), j) = 1}^k c_j} \\ &\geq \frac{1}{n}(m)_k - (c + (m - c)) \sum_{i | e(G), \mu(i) = -1} \frac{1}{i} + k - 1)_k, \end{aligned}$$

where the last equality follows directly from Lemma 2.6.

7. THE CASE $f(x) = x$, $R = G$ AND $D = G$

Proof of Theorem for $D = R = G$. The proof is quite similar as the last case. In this case, $|D| = |G| = m$ and $c = 0$. Applying Lemma 3.1, we have

$$k!N(D, k, b) = \frac{1}{n}(n)_k + \frac{1}{n} \sum_{\psi \neq \psi_0} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi),$$

where C_k is the set of all conjugacy classes of S_k and $C(\tau)$ counts the number of permutations conjugate to τ , and

$$F_\tau(\psi) = \prod_{i=1}^k \left(\sum_{a \in G} \psi^i(a) \right)^{c_i}.$$

A trivial character sum computation gives

$$F_\tau(\psi) = n^{\sum_{i=1}^k c_i m_i(\psi)} 0^{\sum_{i=1}^k c_i (1-m_i(\psi))},$$

where $m_i(\psi)$ is defined as follows: $m_i(\psi) = 1$ if $\psi^i = 1$ and $m_i(\psi) = 0$ if $\psi^i \neq 1$.

Let $e(G)$ be the exponent of G and so it is also the exponent of \hat{G} . Thus for nontrivial character ψ , $m_i(\psi) = 0$ if $(e(G), i) = 1$. We then have

$$\begin{aligned} k!N(D, k, b) &= \frac{1}{n}(n)_k + \frac{1}{n} \sum_{\psi \neq \psi_0} \psi^{-1}(b) \sum_{\tau=(c_1, c_2, \dots, c_k) \in C_k} \text{sign}(\tau) C(\tau) F_\tau(\psi) \\ &= \frac{1}{n}(n)_k + \frac{1}{n} \sum_{1 \neq d|n} \sum_{\psi, \text{order}(\psi)=d} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) n^{\sum_{i=1}^k c_i m_i(\psi)} 0^{\sum_{i=1}^k c_i (1-m_i(\psi))}. \end{aligned}$$

Since for $\tau = (c_1, c_2, \dots, c_k) \in C_k$, $c_i = 0 \Rightarrow m_i(\psi) = 1$, we have

$$\begin{aligned} k!N(D, k, b) &= \frac{1}{n}(n)_k + \frac{1}{n} \sum_{1 \neq d|n} \sum_{\psi, \text{order}(\psi)=d} \psi^{-1}(b) \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) n^{\sum_{i=1}^k c_i} \\ &= \frac{1}{n}(n)_k + \frac{(-1)^k}{n} \sum_{1 \neq d|n} \sum_{\psi, \text{order}(\psi)=d} \psi^{-1}(b) \sum_{\tau \in C_k} (-1)^{c_1+c_2+\dots+c_k} C(\tau) n^{\sum_{i=1}^k c_i} \\ &= \frac{1}{n}(n)_k + \frac{(-1)^k}{n} \sum_{1 \neq d|n} \sum_{\psi, \text{order}(\psi)=d} \psi^{-1}(b) \sum_{\tau \in C_k} C(\tau) (-n)^{\sum_{i=1}^k c_i} \end{aligned}$$

From the formula given in Lemma 2.7, one has

$$\begin{aligned} &\sum_{\tau=(c_1, \dots, c_k) \in C_k} C(\tau) (-n)^{\sum c_i} \\ &= \left[\frac{t^k}{k!} \right] \frac{1}{(1-t^d)^{-n/d}} = \binom{-n/d + k/d - 1}{k/d} = (-1)^{k/d} \binom{n/d}{k/d}. \end{aligned}$$

We then have

$$\begin{aligned} k!N(D, k, b) &= \frac{1}{n}(n)_k + \frac{(-1)^k}{n} \sum_{1 \neq d|n, d|k} \sum_{\psi, \text{order}(\psi)=d} \psi^{-1}(b) k! (-1)^{k/d} \binom{n/d}{k/d} \\ &= \frac{1}{n}(n)_k + \frac{(-1)^k}{n} \sum_{1 \neq d|(n, k)} k! (-1)^{k/d} \binom{n/d}{k/d} \sum_{\psi, \text{order}(\psi)=d} \psi^{-1}(b). \end{aligned}$$

Thus

$$N(D, k, b) = \frac{1}{n} \binom{n}{k} + \frac{1}{n} (-1)^{k+k/d} \sum_{1 \neq d|(n, k)} \binom{n/d}{k/d} \sum_{\psi, \text{order}(\psi)=d} \psi(b),$$

where $\sum_{\psi, \text{order}(\psi)=d} \psi(b)$ is the Ramanujan sum.

Remark: This approach can be used to give explicit formulas when $G \setminus D$ is a very small constant.

Acknowledgements. The authors wish to thank Professor Richard Stanley for his helpful suggestions.

REFERENCES

- [1] J. Bourgain, *Sum-Product Theorems and Applications*, Additive Number Theory: Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson, 2010.
- [2] J. Bourgain, A. Glibichuk and S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) 73 (2006) 380-398.
- [3] J. Bourgain and S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Math. Acad. Sci. Paris 337 (2003) 75-80.
- [4] Q. Cheng, *Hard problems of algebraic geometry codes*, IEEE Trans. Inform. Theory 54 (2008), 402-406.
- [5] T. Cochrane and Z. Zheng, *On upper bounds of Chalk and Hua for exponential sums*, Proc. Amer. Math. Soc. 129 (2001), 2505-2516.
- [6] T. Cochrane and Z. Zheng, *A survey on pure and mixed exponential sums modulo prime powers*, Number theory for the millennium, I 273-300, AK Peters, Natick, MA, 2002.
- [7] P. Ding and M. Qi, *Further estimate of complete trigonometric sums*, J. Tsinghua Univ. 29 (1989), 74-85.
- [8] P. Erdős and H. Heilbronn, *On the addition of residue classes mod p* , Acta Arith. 9 1964, 149-159.
- [9] D.R. Heath-Brown and S.V. Konyagin, *New bounds for Gauss sums derived from k th powers, and for Heilbronn's exponential sum*, Q. J. Math. 51 (2000) 221-235.
- [10] H. Heilbronn, *Lecture Notes on Additive Number Theory mod p* , California Institute of Technology (1964).
- [11] L.K. Hua, *On an exponential sum*, J. Chinese Math. Soc. 2, (1940). 301-312.
- [12] L.K. Hua, *On exponential sums*, Sci. Record (N.S.) 1 (1957), 1-4.
- [13] L.K. Hua, *Additive Primzahltheorie*, (German) B. G. Teubner Verlagsgesellschaft, Leipzig 1959.
- [14] S. Konyagin, *Estimates for Gaussian sums and Waring's problem modulo a prime*, (Russian) Trudy Mat. Inst. Steklov. 198 (1992), 111-124; translation in Proc. Steklov Inst. Math. 1994, (198), 105-117.
- [15] S. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Tracts in Mathematics, 136. Cambridge University Press, Cambridge, 1999.
- [16] M. Kusters, *The subset sum problem for finite abelian groups*, J. Combin. Theory Ser. A 120 (2013), no. 3, 527530.
- [17] N. Kitchloo and L. Pachter, *An interesting result about subset sums*, MIT unpublished notes, 1994.
- [18] J. Li, *On the Odlyzko-Stanley enumeration problem and Warings problem over finite fields*, J. of Number Theory 133 (2013), 2267-2276.
- [19] J. Li and D. Wan, *On the subset sum problem over finite fields*, Finite Fields & Applications, 14 (2008), 911-929.
- [20] J. Li and D. Wan, *A new sieve for distinct coordinate counting*, Science in China Series A 53 (2010) 2351-2362.
- [21] J. Li and D. Wan, *Counting subsets of finite abelian groups*, J. Combin. Theory Ser. A 19 (2012) 170-182.
- [22] J. Li, D. Wan and J. Zhang, *On the minimum distance of elliptic curve codes*, arXiv:1501.01138, to Appear in ITIS 2015.
- [23] M. Lu, *Estimate of a complete trigonometric sum*, Sci. Sinica Ser. A 28 (1985), 561-578.
- [24] A.M. Odlyzko and R.P. Stanley, *Enumeration of power sums modulo a prime*, J. Number Theory 10 (1978) 263-272.
- [25] R.P. Stanley, *Enumerative combinatorics, Vol. 1*, Second Edition, Cambridge University Press, Cambridge, 1997.
- [26] R.P. Stanley and M. F. Yoder, *A study of Varshamov codes for asymmetric channels*, JPL Technical Report 32-1526, DSM, Vol. XIV (1973), 117-123.
- [27] S.B. Stečkin, *An estimate of a complete rational trigonometric sum*, (Russian) Analytic number theory, mathematical analysis and their applications (dedicated to I. M. Vinogradov on his 85th birthday). Trudy Mat. Inst. Steklov. 143 (1977), 188C207, 211.

- [28] D. Wan, *Generators and irreducible polynomials over finite fields*, Mathematics of Computation, Vol. 66, (1997), 1195-1212.
- [29] J. Zhang, F. Fu and D. Wan, *Stopping sets of algebraic geometry codes*, IEEE Transactions On Information Theory, Vol. 60, No. 3, March 2014, 1488-1495.
- [30] G. Zhu and D. Wan, *An asymptotic formula for counting subset sums over subgroups of finite fields*, Finite Fields and Their Applications 18 (2012) 192-209.
- [31] G. Zhu and D. Wan, *Computing the error distance of Reed-Solomon codes*, TAMC 2012 (Theory and Applications of Models of Computation), LNCS, Vol 7287 (2012), 214-224.

DEPARTMENT OF MATHEMATICS, SHANGHAI JIAO TONG UNIVERSITY, SHANGHAI, P.R. CHINA,
DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA
02139-4307, USA

E-mail address: `jiyouli@mit.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, IRVINE, CA 92697-3875, USA

E-mail address: `dwan@math.uci.edu`